CLAIMS

What is claimed is:

1. A circuit for generating a cipher stream, the circuit comprising:

a first and a second plurality of linear feedback shift registers (LFSR),

a first of the second plurality of LFSR having a clock signal as a clock input and others of the first plurality of LFSR having an output of another of the first plurality of LFSR as a clock input;

a first of the first plurality of LFSR having the clock signal combined with an output of the first of the second plurality of LFSR as a clock input and others of the second plurality of LFSR having an output of one of the first plurality of LSFR combined with an output of another of the first plurality of LFSR as a clock input; and

an output of a last of the first plurality of LFSR and an output of a last of the second plurality of LFSR being combined to produce the cipher stream.

2. The circuit of claim 1 wherein the first plurality of LFSR numbers a same value as the second plurality of LFSR.

3. The circuit of claim 1 wherein the combining of the output of one of the first plurality of LSFR with an output of another of another of the first plurality of LSFR is by an AND gate.

4. The circuit of claim 1 wherein the output of the last of the first plurality of LFSR and the output of the last of the second plurality of LFSR is by an exclusive-or gate.

5. Software configured to produce a cipher stream, the software effectively modeling a circuit having components comprising:

a first and a second plurality of linear feedback shift registers (LFSR), a first of the second plurality of LFSR having a clock signal as a clock input and others of the first plurality of LFSR having an output of another of the first plurality of LFSR as a clock input;

a first of the first plurality of LFSR having the clock signal combined with an output of the first of the second plurality of LFSR as a clock input and others of the second plurality of LFSR having an output of one of the first plurality of LSFR combined with an output of another of the first plurality of LFSR as a clock input; and

an output of a last of the first plurality of LFSR and an output of a last of the second plurality of LFSR being combined to produce the cipher stream.

6. The software of claim 5 wherein the first plurality of LFSR numbers a same value as the second plurality of LFSR.

7. The software of claim 5 wherein the combining of the output of one of the first plurality of LSFR with an output of another of another of the first plurality of LSFR is by an AND gate.

8. The software of claim 5 wherein the output of the last of the first plurality of LFSR and the output of the last of the second plurality of LFSR is by an exclusive-or gate.